

1. A system for conducting an agreement between two parties relying on a trusted a third party comprising:

a first party generating a first view of the agreement and transmitting the first view of the agreement to the third party;

a second party independently generating a second view of the agreement and transmitting the second view of the agreement to the third party;

a wireless network connecting the first party and the second party, and

a wired or wireless network connecting the second party to the third party; wherein the trusted third party, receiving the first view of the agreement and the second view of the agreement, verifying conditions including that the identities of the parties that transmitted the agreements and that the independent views of the agreement are consistent with each other and takes action to execute the agreement if the conditions are satisfied.

2. A system as in Claim 1 wherein the agreement pertains to the ordering and or purchasing of goods and services, the first party is a consumer, the second party is a merchant and the third party is a Secure Transaction Server entity.

3. A system as in Claim 2 wherein the generation of views by each party and the verification procedure is based on a secure, symmetric agreement verification protocol.

4. A system as in claim 3 wherein the secure, symmetric agreement verification protocol is the Secure Transaction Protocol.

5. A system of claim 4, further comprising one or more payment service devices and wherein:

the first party comprises a consumer operating a mobile device with an associated identification number;

the second party comprises a merchant operating a device with an associated identification number;

the third party operating a trusted secure transaction server device;

the wireless communication network is in communication with the consumer device and the merchant device;

the wired or wireless communication network is in communication with the merchant device and the trusted secure transaction server device,

and wherein the consumer device, the merchant device, and the trusted secure transaction server device are capable of executing the Secure Transaction Protocol.

6. A system as Claim 4, where the consumer is connected to the merchant via a wireless local area network.

7. The system as in claim 6, wherein the consumer and the merchant do not trust each other and the wireless local area network is open and not secure and the secure transaction server is able to verify the identity of the agreement parties and purchase agreement details.

8. The system as in claim 7 wherein the mobile device stores no personal identifying information about the consumer or account information of the consumer and such account information of the merchant and the consumer is stored in the trusted secure transaction server or is accessible by the secure transaction server.

9. The system as in claim 8, further comprising one or more payment services which execute a payment upon direction of the trusted secure transaction server, wherein the trusted secure transaction server is in secure communication with one or more payment services, including online payment services, financial institutions, and credit card agencies, using a wired or wireless network and the trusted secure transaction server directs that payment be executed by the payment services upon validation of the purchase transaction by the trusted secure transaction server.

10. The system as in claim 9, wherein consumer identifying information and merchant identifying information is stored only in the trusted secure transaction server, and, for authorization by the trusted secure transaction server, the merchant enters merchant identifying information into the merchant device and the consumer enters consumer identifying information into the consumer device.

11. The system as in claim 10, wherein the purchase transaction is for goods and services and the trusted secure transaction server supplies a token as confirmation of payment.

12. The system as in claim 11, wherein the consumer presents the token to the merchant in order to consume a service.

13. The system as in claim 12, wherein only the trusted secure transaction server, and neither the merchant nor the consumer are able to observe details of the other's transaction or identity information.

14. The system as in claim 13, wherein the consumer may be required to authenticate himself to the consumer device, prior to using the device, by entering a personal identifying information, including but not limited to a PIN, password, or by providing biometric authentication, including, but not limited to a fingerprint or a voiceprint.

15. The system as in claim 14, wherein the consumer only authorizes payment through an explicit command to their device, by entering a personal identifying information, including but not limited to a PIN, password, or by providing biometric authentication, including, a fingerprint or a voiceprint.

16. The system as in claim 15, wherein the consumer can select from among financial accounts of the consumer from information stored at the trusted secure transaction server or accessible by the secure transaction server, in order to use the selected account for payment.

17. The system as in claim 16, wherein the consumer and the merchant execute a registration process with the trusted third party by securely providing account information to the trusted secure transaction server and obtaining software to execute the Secure Transaction Protocol, and said registration procedure occurring prior to executing a purchasing transaction and said registration procedure includes providing account information and a unique identifier of the respective consumer operated device or merchant operated device and receive from the trusted secure transaction server device a personal identifying information, such as a PIN, to be only used with the respective consumer operated device or merchant operated device.

18. A system as in claim 17 wherein the conducting of purchase agreements, comprises:
discovering the merchant device by the consumer operating the mobile device;
selecting, by the consumer, goods or services to purchase;
obtaining, from the merchant device, a purchase order;
authorizing, by the consumer, the payment for the purchase order through the consumer device;
authorizing, by the merchant through the merchant device, acceptance of the payment;
verifying by a trusted secure transaction server, identities of the merchant and the consumer and details of the transaction;
causing, by the trusted secure transaction server, payment from the consumer to the merchant through a payment service; and
issuing, by the trusted secure transaction server, receipts to the consumer device and to the merchant device indicating success or failure of the transaction.

19. A system of claim 18, wherein the operator of the trusted secure transaction server collecting a fee for processing a transaction from one or more of the consumer, merchant, payment services, credit card issuers and financial accounts based on a fee for each transaction or on a percentage of transaction amount.

20. The system as in claim 18, further comprising a secure network coupling the merchant operated device with the trusted secure transaction server and wherein the wireless local area network is operated by the merchant operated device.

21. The system as in claim 18, further comprising a secure network coupling the merchant operated device with the trusted secure transaction server and wherein the wireless local area network includes a hotspot accessible by a plurality of merchants and consumers and at which the consumer can select and access the merchant through the wireless local area network.

22. The system as in claim 18, wherein the wireless local area network includes a hotspot accessible by a plurality of merchants and consumers and at which the consumer can select and access the merchant through the wireless local area network and a directory.

23. The system as in claim 18, wherein the wireless local area network includes a hotspot accessible by a plurality of merchants and consumers and at which the consumer can select and access the merchant through the wireless local area network, and wherein the merchant device, the consumer device, and the trusted secure transaction server are in communication with each other via the hotspot.

24. The system as in claim 18, wherein the merchant device executing a retail application and a secure transaction purchasing application, can execute the secure transaction application on a local device at the merchant location connected to the wireless local area network and a remote device connected via another network to the wireless local area network and the consumer device.

25. The system as in any one of claims 19, 20, 21, 22, 23, and 24, wherein the merchant device is connected to the trusted secure transaction server via the Internet using additional security including but not limited to the secure socket layer (SSL) or a Virtual Private Network.

26. The system as in any one of claims 19, 20, 21, 22, 23, and 24, wherein the trusted secure transaction server is connected to one or more payment services through a secure network or through the Internet using additional security including but not limited to the secure socket layer (SSL) or a Virtual Private Network.

27. The system as in claim 18 where a consumer can request that the Secure Transaction Server disable the device and thereby not permitting further transactions for that device with the current personal identification information.

28. The system as in claim 18 where the Secure Transaction Server can detect and disable a consumer account if there are multiple attempts to authorize a payment with incorrect personal identifying information.

29. The system as in claim 18, wherein the consumer can purchase a service, including a movie ticket, from the merchant using a mobile device; receive an electronic token as proof of payment; and the consumer can present the token to obtain the service using their mobile device, including a paperless e-ticket.

30. The system as in claim 18 where the transaction is a return of goods and services from the consumer to the merchant and the secure transaction server will cause payment from the merchant to the consumer.

31. The system as in claim 18 in which the Secure Transaction Server provides ancillary information from the payment services, including but not limited to, advertisements, special interest rate for a particular purchase if a specific credit account is chosen for the attempted purchase, to the consumer in the response messages prior to the final purchasing authorization by the consumer.